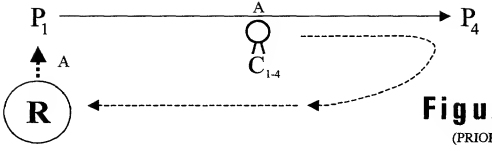


Figure 1
(PRIOR ART)

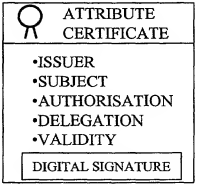
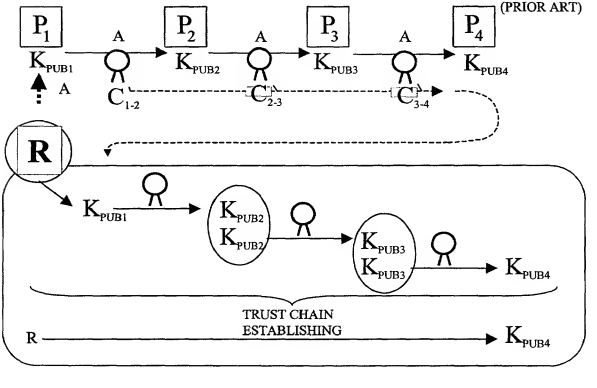


Figure 2
(PRIOR ART)

Figure 3
(PRIOR ART)



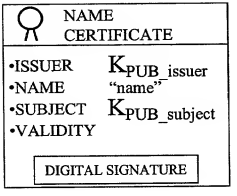


Figure 4
(PRIOR ART)

$$K_{PUB\_issuer} \bullet \text{"name"} = K_{PUB\_subject}$$

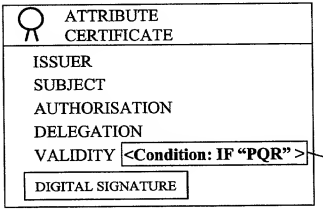
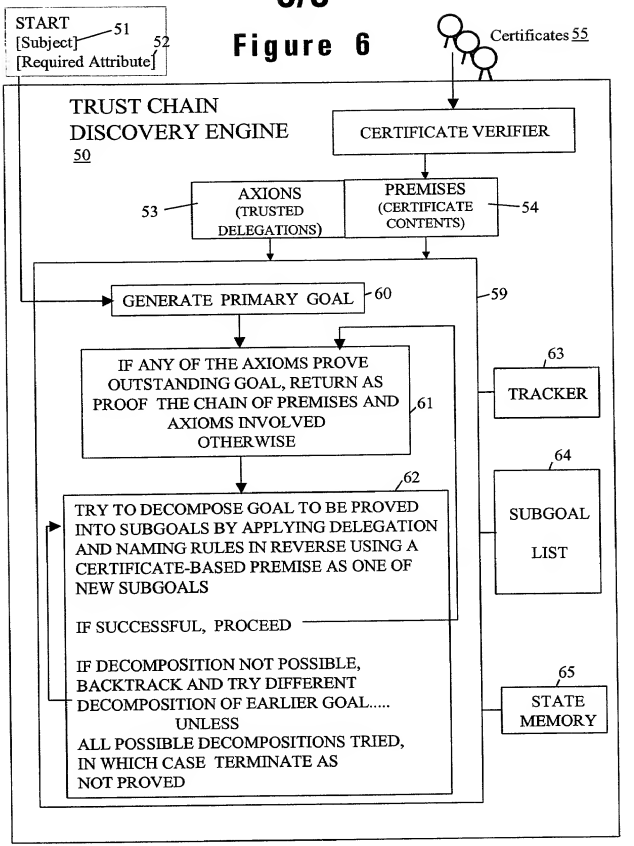


Figure 5

Figure 6


START
[Subject] 51
[Required Attribute] 52
Certificates 55
TRUST CHAIN
DISCOVERY ENGINE
50
CERTIFICATE VERIFIER
53
AXIONS
(TRUSTED
DELEGATIONS)
PREMISES
(CERTIFICATE
CONTENTS)
54
59
GENERATE PRIMARY GOAL
60
IF ANY OF THE AXIOMS PROVE
OUTSTANDING GOAL, RETURN AS
PROOF THE CHAIN OF PREMISES AND
AXIOMS INVOLVED
OTHERWISE
61
63
TRACKER
64
SUBGOAL
LIST
62
TRY TO DECOMPOSE GOAL TO BE PROVED
INTO SUBGOALS BY APPLYING DELEGATION
AND NAMING RULES IN REVERSE USING A
CERTIFICATE-BASED PREMISE AS ONE OF
NEW SUBGOALS
IF SUCCESSFUL, PROCEED
IF DECOMPOSITION NOT POSSIBLE,
BACKTRACK AND TRY DIFFERENT
DECOMPOSITION OF EARLIER GOAL.....
UNLESS
ALL POSSIBLE DECOMPOSITIONS TRIED,
IN WHICH CASE TERMINATE AS
NOT PROVED
65
STATE
MEMORY

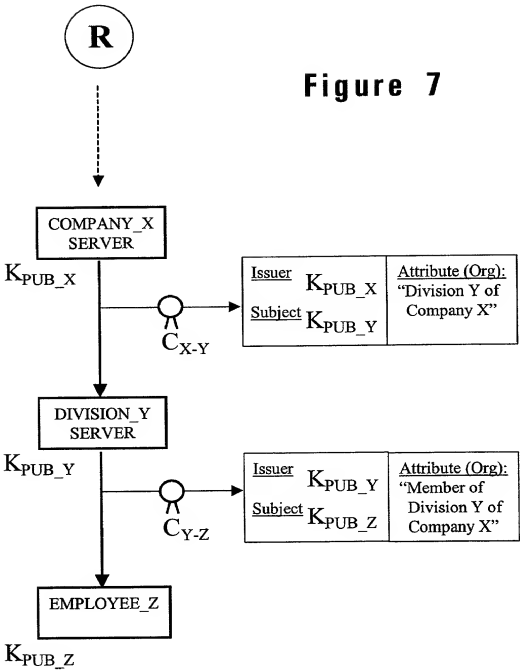

R
COMPANY_X SERVER
K_{PUB_X}
C_{X-Y}
Issuer K_{PUB_X}
Subject K_{PUB_Y}
Attribute (Org): "Division Y of Company X"
DIVISION_Y SERVER
K_{PUB_Y}
C_{Y-Z}
Issuer K_{PUB_Y}
Subject K_{PUB_Z}
Attribute (Org): "Member of Division Y of Company X"
EMPLOYEE_Z
K_{PUB_Z}

Figure 7

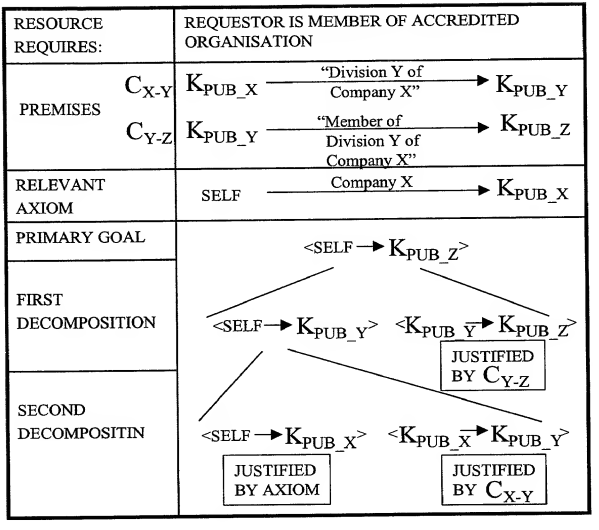

RESOURCE REQUIRES:
REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES
C_{X-Y}
K_{PUB_X} "Division Y of Company X" K_{PUB_Y}
C_{Y-Z}
K_{PUB_Y} "Member of Division Y of Company X" K_{PUB_Z}
RELEVANT AXIOM
SELF Company X K_{PUB_X}
PRIMARY GOAL
<SELF → K_{PUB_Z}>
FIRST DECOMPOSITION
<SELF → K_{PUB_Y}>
<K_{PUB_Y} → K_{PUB_Z}>
JUSTIFIED BY C_{Y-Z}
SECOND DECOMPOSITIN
<SELF → K_{PUB_X}>
JUSTIFIED BY AXIOM
<K_{PUB_X} → K_{PUB_Y}>
JUSTIFIED BY C_{X-Y}

Figure 8

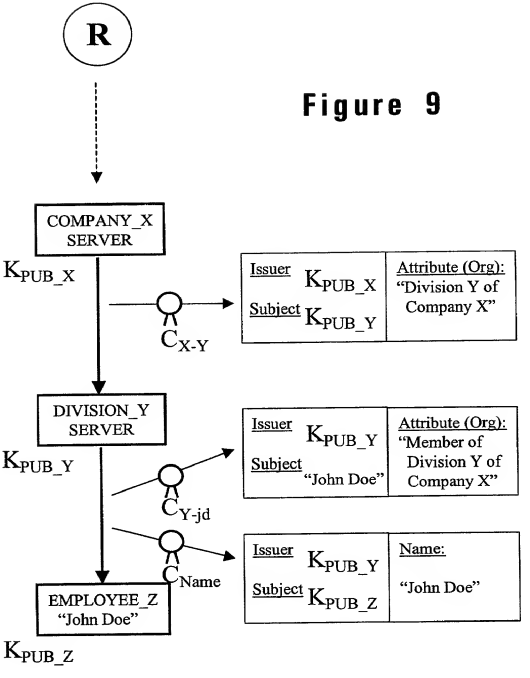

R
COMPANY_X SERVER
K_{PUB_X}
C_{X-Y}
Issuer K_{PUB_X}
Subject K_{PUB_Y}
Attribute (Org): "Division Y of Company X"
DIVISION_Y SERVER
K_{PUB_Y}
C_{Y-jd}
Issuer K_{PUB_Y}
Subject "John Doe"
Attribute (Org): "Member of Division Y of Company X"
C_{Name}
Issuer K_{PUB_Y}
Subject K_{PUB_Z}
Name: "John Doe"
EMPLOYEE_Z "John Doe"
K_{PUB_Z}

Figure 9

RESOURCE REQUIRES:	REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES	$C_{X\text{-}Y}$ $K_{PUB\_X} \xrightarrow{\text{"Division Y of Company X"}} K_{PUB\_Y}$ $C_{Y\text{-}jd}$ $K_{PUB\_Y} \xrightarrow{\text{"Member of Division Y of Company X"}} \text{"John Doe"}$ C_{Name} $K_{PUB\_Y} \cdot [\text{"John Doe"}] = K_{PUB\_Z}$
RELEVANT AXIOM	SELF $\xrightarrow{\text{Company X}} K_{PUB\_X}$
PRIMARY GOAL	<SELF → K_{PUB_Z}>
FIRST DECOMPOSITION	<SELF → "John Doe" ><"John Doe" → K_{PUB_Z}> JUSTIFIED BY C_{Name}
SECOND DECOMPOSITION	<SELF → K_{PUB_Y}> <K_{PUB_Y} → "John Doe" > JUSTIFIED BY $C_{Y\text{-}jd}$
THIRD DECOMPOSITION	<SELF → K_{PUB_X}> <K_{PUB_X} → K_{PUB_Y}> JUSTIFIED BY AXIOM JUSTIFIED BY $C_{X\text{-}Y}$

Figure 10

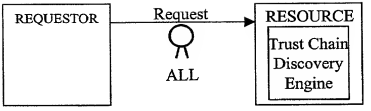


Figure 11

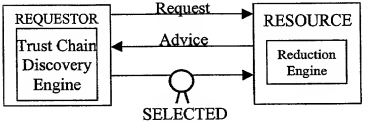


Figure 12

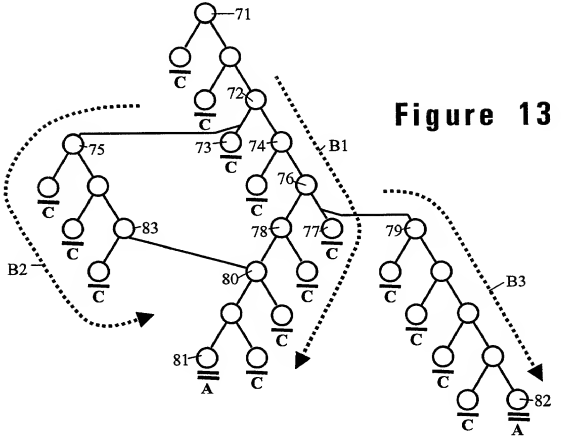


Figure 13